

## Software Maintenance Release Note

# Version 276-03

### for AT-8900 and AT-9900 series switches

This software maintenance release note lists the issues addressed and enhancements made in Maintenance Version 276-03 for Software Release 2.7.6. Release details are listed in the following table:

Models	Series	Release File	Date	Size (bytes)	GUI file
AT-8948	AT-8900	89276-03.rez	4 August 2006	4572948	—
AT-9924T, AT-9924SP, AT-9924T/4SP	AT-9900	89276-03.rez	4 August 2006	4572948	d9924e27.rsc

**Caution:** Using a maintenance version on the wrong model may cause unpredictable results, including disruption to the network.

This maintenance release note should be read in conjunction with the following documents:

- **Release Note for Software Version 2.7.6** for AT-8800, Rapier i, AT-8700XL, AT-8600, AT-9900, AT-8900 and AT-9800 Series Switches and AR400 and AR700 Series Routers (document number C613-10462-00 Rev A)
- your switch's **Document Set for Software Release 2.7.5**. This document set is available on the CD-ROM that shipped with your switch, or from:  
[www.alliedtelesyn.co.nz/documentation/documentation.html](http://www.alliedtelesyn.co.nz/documentation/documentation.html)

**Caution:** Information in this release note is subject to change without notice and does not represent a commitment on the part of Allied Telesis Inc. While every effort has been made to ensure that the information contained within this document and the features and changes described are accurate, Allied Telesis Inc. can not accept any type of liability for errors in, or omissions arising from the use of this information.

## Enabling and Installing this Release

---

To use this maintenance release you must have a base release license for Software Release 2.7.6. Contact your distributor or reseller for more information. To enable this release and install it as the preferred release, use the commands:

```
enable rel=89276-03.rez num=2.7.6
set install=pref rel=89276-03.rez
```

## Levels

---

Some of the issues addressed in this Maintenance Version include a level number. This number reflects the importance of the issue that has been resolved. The levels are:

- Level 1**     This issue will cause significant interruption to network services, and there is no work-around.
- Level 2**     This issue will cause interruption to network service, however there is a work-around.
- Level 3**     This issue will seldom appear, and will cause minor inconvenience.
- Level 4**     This issue represents a cosmetic change and does not affect network operation.

## Features in 276-03

Software Maintenance Version 276-03 includes all resolved issues and enhancements in earlier versions, and the resolved issues and enhancements in the following tables. In the tables, for each product series:

- “Y” indicates that the resolution is available in Version 276-03 for that product series.
- “-” indicates that the issue did not apply to that product series.

### Level 1

CR	Module	Level	Description	AR44x / AR450	AR7x5	AR750S	Rapier i	AT-8800	AT-8600	AT-8700XL	AT-8948	AT-9900	AT-9800
CR00012654 CR00013388	Switch	1	Under heavy CPU utilisation, particularly when many SFPs were installed, AT-9924SP switches sometimes did not correctly detect the installed status of SFPs or reflect the correct link state.  This issue has been resolved. The switch now reports the correct state once the heavy load is removed.	-	-	-	-	-	-	-	-	Y	-

### Level 2

No level 2 issues

### Level 3

No level 3 issues

### Level 4

No level 4 issues

## Enhancements

No enhancements

## Features in 276-02

Software Maintenance Version 276-02 includes all resolved issues and enhancements in earlier versions, and the resolved issues and enhancements in the following tables. In the tables, for each product series:

- “Y” indicates that the resolution is available in Version 276-02 for that product series.
- “-” indicates that the issue did not apply to that product series.

### Level 1

CR	Module	Level	Description	AR44x / AR450	AR7x5	AR750S	Rapier i	AT-8800	AT-8600	AT-8700XL	AT-8948	AT-9900	AT-9800
CR00011691	Switch	1	Previously, if trunk ports were configured and/or STP was enabled, the CPU flooded GARP frames in an incorrect manner, which could cause network loops. This issue has been resolved. GMRP frames are (correctly) flooded, and GVRP frames are now only flooded if GARP is disabled.	-	-	-	Y	Y	Y	Y	Y	Y	-
CR00011694	Core, Switch	1	If the switch had learned a very large number of routes from BGP and the interface went down, IP ran out of memory when recalculating the best routes to use. This was exacerbated when the high memory usage triggered the BGP backoff mechanism which in turn disabled the BGP peers, which caused IP to recalculate even more routes. The switch eventually rebooted due to memory exhaustion. This issue has been resolved by improvements to memory allocation and IP route queuing, and by enforcing limits on the number of IP routes.	-	-	-	Y	Y	-	-	Y	Y	Y
CR00012097	Switch	1	When PIM6 was configured on the switch, and it received an IPv6 multicast stream for which it had no downstream interface to forward the stream to, a reboot could occur. This issue has been resolved.	-	-	-	Y	Y	-	-	Y	Y	Y

## Level 2

CR	Module	Level	Description	AR44x / AR450	AR7x5	AR750S	Rapier i	AT-8800	AT-8600	AT-8700XL	AT-8948	AT-9900	AT-9800
CR00000529	IPv6, PIM6	2	When a better route for multicast traffic became available, PIM for IPv6 did not recalculate the route and switch the traffic to use it.  This issue has been resolved.	Y	Y	Y	Y	Y	-	-	Y	Y	Y
CR00006475	IP Gateway, PIM	2	When PIM-DM or PIM-SM was forwarding traffic through the CPU at high data rates and an SG entry was deleted, it was possible for the router or switch to reboot.  This issue has been resolved.	Y	Y	Y	Y	Y	-	-	Y	Y	Y
CR00007522	IP Gateway	2	The switch's hardware IP route table occasionally did not contain the most optimal route to a destination. This meant packets were sometimes sent via sub-optimal routes. An additional effect was that when multiple equal-cost routes existed a less than complete set of those routes would be utilised.  This issue has been resolved, so that the switch forwards packets via the best IP route(s) available.	-	-	-	Y	Y	Y	Y	Y	Y	Y
CR00007741	TCP, TPAD	2	TPAD TCP sessions now have a keepalive timer applied to them. If a TPAD TCP session is inactive and therefore there is no response to the TCP keepalives, then after 3 keepalive attempts, 10 seconds apart, the TPAD TCP session is closed. This frees up the TCP listen port to allow subsequent TPAD transactions via that TCP port. This TCP keepalive facility only applies to TPAD-related TCP traffic.	Y	Y	Y	Y	-	-	-	-	-	-
CR00007950	SSH	2	When a user is logged into the router or switch via an ASYN port and uses the SSH client to send a command to a remote SSH server, the server sends the response and the SSH session is closed as expected. However, the tail end of the response was sometimes not received by the user logged into the ASYN port.  This issue has been resolved.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y

CR	Module	Level	Description	AR44x / AR450	AR7x5	AR7505	Rapier i	AT-8800	AT-8600	AT-8700XL	AT-8948	AT-9900	AT-9800
CR00008699	Switch	2	Previously, when 300 MAC address filters were added to a port and the port was reset, the CPU became 100% utilised. This issue has been resolved.	-	-	-	Y	Y	Y	Y	-	-	-
CR00008992	IPv6	2	The router or switch sometimes unexpectedly stopped forwarding IPv6 multicast traffic if the multicast's upstream path changed. This could occur, for example, when the path changed because an interface went down.	Y	Y	Y	Y	Y	-	-	Y	Y	Y
CR00009201	ARP	2	An ARP timeout caused the removal of the ARP entry, resulting in packet loss until the entry was re-added. This issue has been resolved.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR00009280	ATM	2	When the router was using IPsec and either IPoEoA or IPoA, and it received traffic from a VLAN at a higher rate than it could transmit over the ADSL link, eventually the ATM interface would intermittently stop transmitting traffic. This issue has been resolved.	Y	-	-	-	-	-	-	-	-	-
CR00009283	Switch	2	If a 48-port switch learned many thousands of MAC addresses, it rebooted when the addresses timed out. This issue has been resolved.	-	-	-	Y	Y	Y	Y	-	-	-
CR00009539	IP Gateway	2	The IP DNS cache feature was not designed to include MX (Mail Exchange) DNS records. In some circumstances, MX DNS entries were added to the IP DNS cache and the name of a DNS record was incorrectly associated with the IP address of the MX entry. This stopped the router or switch from correctly resolving A-record requests for the affected domain name. This issue has been resolved by ensuring that MX entries are never added to the IP DNS cache.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR00010265	Switch	2	When the ingress and egress port were defined in an Layer 3 filter with an action of <b>deny</b> , the filter denied the traffic to be sent out all the egress ports and not just the egress port specified in the filter. This issue has been resolved.	-	-	-	Y	Y	Y	Y	-	-	-

CR	Module	Level	Description	AR44x / AR450	AR7x5	AR750S	Rapier i	AT-8800	AT-8600	AT-8700XL	AT-8948	AT-9900	AT-9800
CR00010886	IPv6, IP Gateway, PPP	2	When a user enabled a Dial-on-Demand PPP interface, sometimes the router or switch did not apply the associated IP route change. This meant that routes via the Dial-on-Demand PPP interface were not available for use. When this occurred, routed traffic failed to activate the associated Dial-on-Demand PPP interface.  This issue has been resolved.	Y	Y	Y	Y	Y	-	-	Y	Y	Y
CR00011060	IP Gateway, PIM	2	In networks with redundancies handled by protocols such as STP and trunking, upstream PIM neighbours may move from one port to another. When this happened, PIM-DM failed to re-establish multicast routes with all of its downstream interfaces listed properly. This caused the switch to eventually stop sending multicasts for that group via that route.  This issue has been resolved.	-	-	-	Y	Y	-	-	Y	Y	Y
CR00011128	BGP	2	When running a BGP network using route reflectors, changing the cluster ID on a router or switch could cause a restart of some of the BGP clients.  This issue has been resolved.	Y	Y	Y	Y	Y	-	-	Y	Y	Y
CR00011304	VRRP	2	VRRP did not function correctly when the switch was configured with protected VLANs.  This issue has been resolved.	-	-	-	Y	Y	Y	Y	-	-	-
CR00011305	IPv6, Utility	2	RIPng (RIPv6) occasionally advertised sub-optimal routes to its neighbour when the router or switch was placed in a looped network topology.  This issue has been resolved.	Y	Y	Y	Y	Y	-	-	Y	Y	Y
CR00011338	ASYN	2	If a cable carrying a continuous stream of characters is connected to a port on an 4-port ASYN PIC, the ASYN port did not always receive the characters correctly. This was because of a port synchronisation failure to the character stream.  This issue has been resolved. The port now detects the synchronisation failure and continues to attempt synchronisation to the character stream until successful.	Y	Y	Y	Y	-	-	-	-	-	-

CR	Module	Level	Description	AR44x / AR450	AR7x5	AR750S	Rapier i	AT-8800	AT-8600	AT-8700XL	AT-8948	AT-9900	AT-9800
CR00011349	SYN	2	At low baud rates, a synchronous connection was unable to reach 100% utilisation of the available bandwidth. The queueing mechanism has been improved to allow 100% link utilisation. Flag sharing between back-to-back HDLC frames is now supported for synchronous connections.	Y	Y	Y	Y	-	-	-	-	-	-
CR00011396	PIM on IPv6	2	When a user specified a static RP candidate and saved the configuration with the <b>create config</b> command, the resulting configuration file did not include the RP candidate. Therefore, rebooting the router or switch deleted the static RP candidate entry.  This issue has been resolved.	Y	Y	Y	Y	Y	-	-	Y	Y	Y
CR00011411	PoE	2	When multiple telnet sessions were open on the AT-8624PoE switch, and the command <b>show switch port</b> was entered, the switch command line became unresponsive for several minutes.  This issue has been resolved.	-	-	-	-	-	Y	-	-	-	-
CR00011586	Switch	2	When a port is no longer a member of any VLAN as an untagged port, it would discard received untagged BPDU packets.  Note that this issue only occurred on AT-8900 and AT-9900 switches; other switches already correctly handled untagged frames on tagged ports when required.  This issue has been resolved.	-	-	-	-	-	-	-	Y	Y	-
CR00011587	Switch	2	Previously, if a port was a tagged member of a VLAN, it was not able to transmit untagged frames to that VLAN.  This issue has been resolved. When required, STP BPDUs can now be sent untagged out a port, even if the port is configured as a tagged member of a VLAN.	-	-	-	-	-	-	-	Y	Y	-
CR00011645	Switch	2	After an AT-8800 series switch was powered down or rebooted, non auto-negotiating copper GBICs did not correctly handle Ethernet PAUSE frames.  This issue has been resolved.	-	-	-	-	Y	-	-	-	-	-



CR	Module	Level	Description	AR44x / AR450	AR7x5	AR7505	Rapier i	AT-8800	AT-8600	AT-8700XL	AT-8948	AT-9900	AT-9800
CR00011665	PRI	2	When using an unstructured TDM group over an E1 mode PRI interface, occasionally a high level of errors was experienced. This may have caused the link to be unstable, or may have resulted in reduced data throughput. This issue has been resolved.	Y	Y	Y	Y	-	-	-	-	-	-
CR00011746	BGP	2	If the router or switch failed to establish a BGP peer session because of unsuccessful Open message exchanges, no further attempts to establish the peer connection were made. This issue has been resolved. The router or switch now continues to attempt to establish the session, with 60 second intervals between attempts.	Y	Y	Y	Y	Y	-	-	Y	Y	Y
CR00011780	BOOTP	2	Previously, if a user entered the command <b>set bootp relay option82 port=portnum</b> without also specifying one of the required <b>subscriberid</b> or <b>trusted</b> parameters, the router or switch would incorrectly report "Operation Successful". This issue has been resolved. The router or switch now reports that one of the parameters <b>subscriberid</b> or <b>trusted</b> must also be specified as part of this command.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR00011809	Firewall	2	The SIP application layer gateway (ALG) did not correctly handle SIP packets that had an extension parameter added to the "From" field. In VoIP networks that added this extension parameter, users telephoning out from the private network could not hear the recipient talk, because the VoIP voice data was not passed from the remote client to the client on the private side. This issue has been resolved.	Y	Y	Y	Y	Y	-	-	-	-	Y
CR00011844	IPv6	2	IPv6 interfaces did not work over a PPP link on switches or AR44x routers. When the interface received IPv6 traffic, the router or switch rebooted. This issue has been resolved.	Y	-	-	Y	Y	-	-	Y	Y	Y

CR	Module	Level	Description	AR44x / AR450	AR7x5	AR7505	Rapier i	AT-8800	AT-8600	AT-8700XL	AT-8948	AT-9900	AT-9800
CR00011855	TCP, UPnP	2	TCP sessions would sometimes “hang” in the Close Wait state. This behaviour occurred when a UPnP notification session was closed by the control point (usually Windows XP, SP2), via a “200 OK” message that contained a “Connection: close” field, that also had the TCP/FIN flag set.  Because these TCP sessions were not closing, eventually all available TCP resources could be used up, preventing new TCP sessions from opening.  This issue has been resolved. Such TCP sessions now close correctly.	Y	Y	Y	-	-	-	-	-	-	-
CR00011940	Switch	2	Previously, if all configured IP interfaces were down or had been deleted, broadcast frames were not sent to the switch’s CPU. This meant, for example, that VLANs on the switch did not receive PPPoE traffic if all IP interfaces were down.	-	-	-	-	-	-	-	Y	Y	-
CR00011991	WAN load balancer	2	An issue occurred when the router accessed multiple WAN load balancer healthcheck hosts, and was configured as a firewall that performed enhanced NAT. Instead of testing the health of each healthcheck host through every WAN LB resource (and therefore over all relevant WAN interfaces), the router only tested through one WAN LB resource. If that one WAN interface lost connectivity to the Internet, the WAN LB incorrectly thought that all WAN LB resources had become unavailable.  This issue has been resolved. The WAN LB now correctly checks the health of all healthcheck hosts through all WAN LB resource interfaces.	Y	Y	Y	-	-	-	-	-	-	-
CR00011992	Firewall	2	When the firewall was enabled, it failed to process some RTSP packets, so clients behind the firewall failed to load some web pages that used RTSP (TCP port 7070).  This issue has been resolved.	Y	Y	Y	Y	Y	-	-	-	-	Y

CR	Module	Level	Description	AR44x / AR450	AR7x5	AR7505	Rapier i	AT-8800	AT-8600	AT-8700XL	AT-8948	AT-9900	AT-9800
CR00012013	VLAN	2	When MLD snooping was enabled and the switch received IPv6 multicast packets (such as MLD Query, Report or Done messages; IPv6 NS packets; and IPv6 RA packets) on a non-master port of a trunk group, it incorrectly forwarded them out the master port. This resulted in a packet loop. This issue has been resolved.	-	-	-	Y	Y	-	-	Y	Y	Y
CR00012067	OSPF	2	A summary LSA was not turned into a route if the destination and mask fell inside one of the router or switch's active ranges, unless it exactly matched the active range's address and mask. This complied with RFC 1583 section 16.2. However, the recommended behaviour has been modified in RFC 2328 section 16.2. To comply with this, the LSA is now calculated if it falls inside one of the router or switch's active ranges.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR00012096	Core, LLDP, Switch, Utility	2	The LLDP module and several monitoring features started up when they were not needed. This impacted on performance. This issue has been resolved, and therefore performance has been improved, especially for the AR440S router.	Y	-	-	-	-	-	-	-	-	-
CR00012108	Switch	2	The command <b>disable switch port=port-number link=disable</b> did not correctly disable the link for port 12 or 24 on AT-9924SP switches. It only disabled ports 12 and 24 in software. This issue has been resolved.	-	-	-	-	-	-	-	-	Y	-
CR00012119	Load balancer	2	Previously, only one <b>resstate</b> trigger could be created for each load balancer resource. This meant, for example, that you could create a trigger to activate a script when a resource went down, but could not activate another script when the resource came back up again. This issue has been resolved. You can now define different triggers to trigger off each of the different states available for a given resource (such as <b>lbstate=up</b> and <b>lbstate=closing</b> ).	Y	Y	Y	Y	Y	-	-	Y	Y	Y

CR	Module	Level	Description	AR44x / AR450	AR7x5	AR7505	Rapier i	AT-8800	AT-8600	AT-8700XL	AT-8948	AT-9900	AT-9800
CR00012140	PIM	2	If the link between two PIM Sparse Mode neighbours was removed, sometimes one of the neighbours rebooted. This issue has been resolved.	Y	Y	Y	Y	Y	-	-	Y	Y	Y
CR00012167	Switch	2	When MAC address entries time out in the switch's ARP table, the switch re-ARPs for the entry's MAC address and adds the entries back if it gets a reply. When 48-port switches re-added the entry, sometimes they associated it with the wrong port number. This stopped the switch from transmitting traffic to that MAC address. This issue has been resolved.	-	-	-	Y	Y	Y	Y	-	-	-
CR00012204	PPP, Eth, IP Gateway, VRRP	2	If VRRP and/or PPP interfaces underwent many state changes, slow memory leaks occurred. This issue has been resolved.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR00012232 CR00012430	Firewall, SIP ALG	2	Some SIP phones may alter or periodically refresh the session information for a call, by sending a re-invite message while the call is in progress. Previously, when a call was established between two SIP phones on the private side of the firewall and one of the phones attempted to update the session information, the call became corrupted. This meant that one of the callers stopped hearing the other. This issue has been resolved.	Y	Y	Y	Y	Y	-	-	-	-	Y
CR00012233	BOOTP	2	When the router or switch acted as a relay agent to process BOOTP requests that contained option 82, it modified the option 82 information of packets even when their giaddr field was set to a non-zero value. The router or switch applied the policy specified by the command: <pre>set bootp relay option82 policy={drop keep replace}</pre> This issue has been resolved. As required by RFC 3046, the router or switch now forwards client DHCP packets that have a non-zero giaddr field without modifying their option 82 fields.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y

CR	Module	Level	Description	AR44x / AR450	AR7x5	AR750S	Rapier i	AT-8800	AT-8600	AT-8700XL	AT-8948	AT-9900	AT-9800
CR00012304	TPAD	2	TPAD previously had issues when the LRC (Longitudinal Redundancy Check) at the end of a transaction was 0x00 <b>and</b> the transaction was via the TCP port. The transaction would stall in the box and eventually time out the X.25 call. This issue has been resolved. TPAD transactions now accept an LRC with a value of 0x00 and operate as normal.	Y	Y	Y	Y	-	-	-	-	-	-
CR00012319	IPv6	2	If the router or switch received a packet that was destined for a link-local address that did not exist, it tried to forward the packet. This caused it to reboot. For example, if a user pinged a non-existent link-local address, the router or switch rebooted. This issue has been resolved by ensuring that the router or switch does not attempt to forward or route packets destined for a link-local interface. Such packets should not be forwarded because they are intended for the local link.	Y	Y	Y	Y	Y	-	-	Y	Y	Y
CR00012396	Firewall, Software QoS	2	When the router or switch was running software QoS and performing NAT through the firewall, it did not check egress classifiers against the pre-NAT address of translated packets. This issue has been resolved.	Y	Y	Y	Y	-	-	-	-	-	-

CR	Module	Level	Description	AR44x / AR450	AR7x5	AR750S	Rapier i	AT-8800	AT-8600	AT-8700XL	AT-8948	AT-9900	AT-9800
CR00012482	Core, Utility, Stacking	2	<p>A few commands on the switch are local commands—they relate only to the switch on which the user types them, and not to any other switch in the stack. The <b>edit</b> command is one such command. Previously, local commands were directed across the stack, which meant they could be sent to other stack members. This caused the following issues with the <b>edit</b> command:</p> <ul style="list-style-type: none"> <li>■ The editing window displayed the command response from other stack members</li> <li>■ If the user closed the file and tried to edit it again, the switch displayed an error message stating that the file was being edited by another user</li> </ul> <p>These issues have been resolved, resulting in the following changes:</p> <ul style="list-style-type: none"> <li>■ Local commands now cannot be host directed. A local command that is host directed will be refused.</li> <li>■ Local commands are not sent to other stack members. Previously, local commands were sent but were not actioned on other stack members—a "not applicable to this host" message informed users of this.</li> <li>■ The command <b>show config dynamic</b> is now a local command.</li> <li>■ The command <b>disable stack</b> cannot be run from a script.</li> </ul>	-	-	-	Y	Y	Y	Y	Y	Y	-
CR00012533	IP Gateway	2	<p>Under some router configurations (for example, WAN load balancing), performing a trace route from a Microsoft Windows PC caused the router to reboot.</p> <p>This issue has been resolved.</p>	Y	Y	Y	-	-	-	-	-	-	-

CR	Module	Level	Description	AR44x / AR450	AR7x5	AR750S	Rapier i	AT-8800	AT-8600	AT-8700XL	AT-8948	AT-9900	AT-9800
CR00012613	Firewall	2	<p>When the WAN load balancer was used with IP NAT (instead of firewall NAT), and an FTP session was established to a server on the public network, the router did not correctly establish a return session. This meant data was unable to flow correctly back from the server, and the router rebooted.</p> <p>This issue has been resolved.</p> <p>Note that the WAN load balancer is not designed for use with IP NAT, because IP NATs are not associated with interfaces. Configurations that use an IP NAT cannot vary the global IP address (the <b>gblip</b> parameter) based on the outgoing interface, so the WAN load balancer sends all traffic out with the same source address. Therefore, the return traffic probably comes back via the WAN load balancer resource that is associated with the global IP. The impact is that the WAN load balancer balances the outgoing traffic but not the return traffic.</p> <p>We recommend using firewall NAT instead of IP NAT with the WAN load balancer.</p>	Y	Y	Y	-	-	-	-	-	-	-
CR00012649	Switch, MLD Snooping	2	<p>The switch sometimes flooded IPv6 multicast traffic undesirably, if the MLD All Routers snooping group contained more than one port and another snooping group contained no ports. In this situation, when a port timed out of the All Routers group, multicast traffic from the empty snooping group was flooded to all ports on the switch. Flooding continued until the last port timed out of the All Routers group.</p> <p>This issue has been resolved.</p>	-	-	-	Y	Y	-	-	Y	Y	Y
CR00012689	IP Gateway, IGMP proxy	2	<p>When IGMP proxy was configured and a user first deleted the upstream interface, then deleted a downstream interface, the router or switch sometimes rebooted. Note that this issue did not occur if the downstream interface was deleted first.</p> <p>This issue has been resolved.</p>	Y	Y	Y	Y	Y	Y	Y	-	-	-

## Level 3

CR	Module	Level	Description	AR44x / AR450	AR7x5	AR750S	Rapier i	AT-8800	AT-8600	AT-8700XL	AT-8948	AT-9900	AT-9800
CR00006900	BGP, IP Gateway	3	If the metric on a blackhole route was changed using the command <b>set ip route</b> and this caused another route, which was being suppressed by the blackhole route, to become preferred, that route could sometimes fail to be imported into BGP.  This issue has been resolved.	-	-	-	-	-	-	-	Y	Y	-
CR00008741	Switch	3	On 48-port switches, when a user created a static MAC address entry on a port (using the <b>add switch filter</b> command) and then entered a learn limit on that port, the static MAC address entry was sometimes deleted.  This issue has been resolved.	-	-	-	Y	Y	Y	Y	-	-	-
CR00009379	Appletalk	3	When the router or switch was using AppleTalk, it occasionally failed to process traffic. When this occurred, entering AppleTalk commands could cause the router or switch to reboot.  This issue has been resolved.	Y	Y	Y	Y	Y	-	-	Y	Y	Y
CR00009918	RSVP	3	When RSVP reserved more than about 30 sessions, the router or switch sometimes rebooted.  This issue has been resolved.	Y	Y	Y	Y	Y	-	-	Y	Y	Y
CR00010080	Classifier	3	If a user defined a classifier to match <b>ethformat=snap-untagged protocol=ip</b> , and used that classifier in a hardware filter to discard matching packets, and saved the configuration, then the classifier in the resulting configuration file did not work properly.  This issue has been resolved.	-	-	-	-	-	-	-	Y	Y	-



CR	Module	Level	Description	AR44x / AR450	AR7x5	AR7505	Rapier i	AT-8800	AT-8600	AT-8700XL	AT-8948	AT-9900	AT-9800
CR00010508	BGP	3	When the router or switch received a BGP update message and created new prefix entries for the routes in the update, it reversed the order of the AS segments. This issue has been resolved.	Y	Y	Y	Y	Y	-	-	Y	Y	Y
CR00010952	IPv6	3	If either of the following were configured for MLD: ■ a <b>qinterval</b> greater than 32 seconds ■ a <b>qinterval</b> greater than 128 seconds then the router or switch sent MLDv2 query packets with incorrect Maximum Response Code and Querier's Query Interval Code fields. This issue has been resolved.	Y	Y	Y	Y	Y	-	-	Y	Y	Y
CR00010953	IPv6	3	Previously, it was possible to enter values for the <b>set ipv6 mld qinterval</b> command that were higher than was specified in RFC 2710. This issue has been resolved. The valid range for <b>qinterval</b> is now 1 to 8387 seconds. Note that if the router or switch acts as an MLDv1 querier and <b>qinterval</b> is set to more than 65 seconds, then the Maximum Response Code in MLDv1 query packets will be set to 65535 milliseconds, because this is the highest valid value for that field.	Y	Y	Y	Y	Y	-	-	Y	Y	Y
CR00011105	IP Gateway	3	Configuring more than about 100 logical IP interfaces decreased the firewall performance. This issue has been resolved. Firewall performance is now very good even when 600 logical IP interfaces are configured.	Y	Y	Y	-	-	-	-	-	-	-
CR00011316		3	Previously, entering the command <b>set summertime</b> could cause extra digits to appear in the output of the commands <b>show ip interface</b> and <b>show config dynam=trigger</b> . This issue has been resolved.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y

CR	Module	Level	Description	AR44x / AR450	AR7x5	AR7505	Rapier i	AT-8800	AT-8600	AT-8700XL	AT-8948	AT-9900	AT-9800									
CR00011510	IPsec	3	The maximum SPI value has been increased in the commands: <pre>create ipsec saspecification=<i>spec-id</i> inspi=<i>spi</i> outspi=<i>spi</i> [<i>other parameters</i>] set ipsec saspecification=<i>spec-id</i> inspi=<i>spi</i> outspi=<i>spi</i> [<i>other parameters</i>]</pre> The <i>spi</i> is now an integer in the range 256 to 4294967295.	Y	Y	Y	Y	Y	-	-	-	-	-									
CR00011659	TTY, VRRP	3	When VRRP debug was enabled from a telnet session, the debugging did not stop when the telnet session closed. If the next telnet session got the same TTY number as the closed session, VRRP debug output was displayed immediately the session started. This made it possible for unauthorised users to view the debug output.  This issue has been resolved.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y									
CR00011687	BOOTP	3	The command <b>set bootp relay maxhops</b> is now supported, in addition to the existing command <b>set bootp maxhops</b> .	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y									
CR00011774	Switch	3	The dot1qTpFdbPort MIB entry displays the ports on which the switch has learned MAC addresses. Previously, the switch started the list of ports at port 0 instead of port 1.  This issue has been resolved.	-	-	-	Y	Y	Y	Y	Y	Y	Y									
CR00011784	IP Gateway	3	If the router received an ARP response for an address outside of the receiving interface's subnet, it discarded the ARP response. This is the intended behaviour on some AR410 routers (see CR00010261) but not on AR7x5 routers.  This issue has been resolved. AR7x5 routers now forward such ARP responses.	-	Y	-	-	-	-	-	-	-	-									
CR00011888	Switch	3	When a trunk group on a 48-port switch spanned multiple switch instances, the switch sometimes did not transmit traffic. The ports in each instance are: <table><tr><td><i>Models</i></td><td><i>First instance</i></td><td><i>Second instance</i></td></tr><tr><td>Rapier 48i, AT-8748XL, AT-8648T/2SP</td><td>1-24, 49</td><td>25-48, 50</td></tr><tr><td>AT-8848</td><td>1-24, 50</td><td>25-48, 49</td></tr></table> This issue has been resolved.	<i>Models</i>	<i>First instance</i>	<i>Second instance</i>	Rapier 48i, AT-8748XL, AT-8648T/2SP	1-24, 49	25-48, 50	AT-8848	1-24, 50	25-48, 49	-	-	-	Y	Y	Y	Y	-	-	-
<i>Models</i>	<i>First instance</i>	<i>Second instance</i>																				
Rapier 48i, AT-8748XL, AT-8648T/2SP	1-24, 49	25-48, 50																				
AT-8848	1-24, 50	25-48, 49																				

CR	Module	Level	Description	AR44x / AR450	AR7x5	AR750S	Rapier i	AT-8800	AT-8600	AT-8700XL	AT-8948	AT-9900	AT-9800
CR00011931	VLAN	3	After users added multiple ports to one private VLAN as tagged ports, those ports could not be added to another private VLAN as tagged ports by using a single command (they could be added one port at a time). This issue has been resolved.	-	-	-	Y	Y	Y	Y	Y	Y	-
CR00011943	IP Gateway	3	Previously, it was possible to modify settings for the default local IP interface when it had no IP address. However, these settings were invalid so the router or switch did not save them. This issue has been resolved. Settings for the default local IP interface now cannot be changed unless the interface has an IP address assigned to it.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR00011969	OSPF	3	When a user changed the <b>asexternal</b> setting for OSPF, sometimes OSPF did not correctly update the LSA database. This issue has been resolved.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR00012014	Switch	3	Setting a port's speed to a fixed speed (such as <b>100mfull</b> ) should also disable <b>automdi</b> on the port. Previously, if the switch set the port speed to a fixed speed during start-up before the switch had fully initialised, auto MDI was not disabled. This issue has been resolved.	-	-	-	-	-	-	-	Y	Y	-
CR00012036	Firewall	3	Previously, the command <b>set firewall policy=policy-name othertimeout=minutes</b> did not change the timeout period for firewall GRE sessions. This issue has been resolved. Note that when a firewall session establishes, its timeout is initially set to 5 minutes. Once the session processes two or more packets, its timeout changes to the value specified by this command.	Y	Y	Y	Y	Y	-	-	-	-	Y

CR	Module	Level	Description	AR44x / AR450	AR7x5	AR750S	Rapier i	AT-8800	AT-8600	AT-8700XL	AT-8948	AT-9900	AT-9800
CR00012040	IP Gateway, WAN load balancer	3	If policy-based routing and the WAN load balancer were both configured, the load balancer balanced traffic even if it matched the routing filter. Because the purpose of policy-based routing is to control the route that traffic uses, this was incorrect.  This issue has been resolved. Traffic that matches a policy-based routing filter now bypasses the WAN load balancer.	Y	Y	Y	-	-	-	-	-	-	-
CR00012175	OSPF	3	In a segmented NBMA network, in which more than one designated router was elected for the network, sometimes the router or switch did not add the routes to the extra designated routers. Note that a segmented network like this only occurs as the result of an incorrect configuration.  This issue has been resolved. The router or switch correctly determines routes in such a network.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR00012265	ATM	3	Previously, ATM interfaces stopped transmitting when any of the following happened: <ul style="list-style-type: none"> <li>■ the command <b>reset pri</b> was entered</li> <li>■ the command <b>reset bri</b> was entered</li> <li>■ more than two ISDN calls were opened (on Software Versions prior to 2.7.6)</li> </ul> This issue has been resolved.	Y	-	-	-	-	-	-	-	-	-
CR00012283	Switch	3	Previously, it was not possible to create two protocol-based VLANs on the same ports if they had the same protocol but a different Ethernet encapsulation.  This issue has been resolved, so you can now create such VLANs.	-	-	-	-	-	-	-	Y	Y	-
CR00012305	QoS	3	When a user entered a <b>maxbandwidth</b> for QoS, the switch sometimes displayed a message that said the bandwidth units were “kbytes” instead of kilobits per second.  This issue has been resolved.	-	-	-	Y	Y	Y	Y	-	-	-

CR	Module	Level	Description	AR44x / AR450	AR7x5	AR7505	Rapier i	AT-8800	AT-8600	AT-8700XL	AT-8948	AT-9900	AT-9800
CR00012307	VLAN	3	Previously, when MSTP was configured it was not possible to delete ports from VLANs in the MSTP CIST, unless MSTP was first disabled. This issue has been resolved. Deleting such ports is now permitted.	-	-	-	Y	Y	Y	Y	Y	Y	-
CR00012314	TACACS+, Telnet	3	If a user connects to the router or switch via telnet and is authenticated using TACACS+, previously the rem_addr field in the TACACS+ packets contained the text "Telnet x" (where x was the number of the telnet session) instead of the remote IP address. This issue has been resolved. The rem_addr field now contains the remote IP address.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR00012322	Classifier	3	If a user created a classifier that specified an IP address without specifying a protocol (for example, <b>create classifier=1 ipda=20.20.20.10/24</b> ), and saved the configuration with the <b>create config</b> command, the resulting configuration file included a value for protocol (for example, <b>create class=1 prot="ip" ipda=20.20.20.10/24</b> ). This prevented the router or switch from applying the classifier to IPsec tunnelled traffic. This issue has been resolved. The protocol value is no longer added to such classifiers, which leaves them matching the default of <b>any</b> .	Y	Y	Y	Y	-	-	-	-	-	-
CR00012329	Asyn	3	When the router sent a continuous stream of data over a permanent assignment, and the ASYN port at the receiving end of the tunnel was significantly slower than the ASYN port at the sending end, the sending router eventually rebooted. This was because the router had to queue packets and eventually ran out of memory. This issue has been resolved. The router now stops receiving ASYN data when memory is low, so its queue does not get too full.	Y	Y	Y	-	-	-	-	-	-	-
CR00012359	Switch	3	You can now return the description of a switch port to its original blank value by entering the following command:  <b>set switch port=port-number description=</b> and providing no value for the <b>description</b> parameter.	Y	-	Y	Y	Y	Y	Y	Y	Y	Y

CR	Module	Level	Description	AR44x / AR450	AR7x5	AR750S	Rapier i	AT-8800	AT-8600	AT-8700XL	AT-8948	AT-9900	AT-9800
CR00012413	Logging	3	When a user creates permanent log filters, the existing default filter is moved to the bottom of the list of filters, instead of being deleted. This behaviour is correct. However, output of the command <b>show config dyn=log</b> previously included commands to delete the default filter then add it back in, which was confusing. This issue has been resolved. The output of the command <b>show config dyn=log</b> now only includes the default filter if the user has specified the default filter in a command. To see all existing filters, use the command <b>show log output=permanent full</b> .	-	Y	-	Y	Y	-	Y	Y	Y	Y
CR00012427	Logging	3	If a user modified the permanent log by destroying it and creating a new one, and then saved the configuration with the command <b>create config</b> , the resulting configuration file included the command <b>destroy log output=permanent</b> . Therefore when the router or switch restarted it destroyed the log and all entries.  This issue has been resolved. The command <b>create config</b> now writes the command <b>set log output=permanent</b> to the configuration file instead of the <b>destroy</b> and <b>create</b> commands.	-	Y	-	Y	Y	-	Y	Y	Y	Y
CR00012468	OSPF	3	An OSPF router or switch could show large numbers of entries in its retransmission lists to certain neighbours under certain conditions (for example, in a congested Frame Relay network). In some cases, the number of items in the list was larger than the number of LSAs in the database.  This issue has been resolved.  Also, a new NRL debugging option has been added to OSPF, to show additions to and deletions from the neighbour retransmission list. To enable NRL debugging, use the command:  enable ospf debug=nrl  Note that this option may generate large amounts of debugging output on a large OSPF network. Use it with care.  To disable NRL debugging, use the command:  disable ospf debug=nrl	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y

CR	Module	Level	Description	AR44x / AR450	AR7x5	AR750S	Rapier i	AT-8800	AT-8600	AT-8700XL	AT-8948	AT-9900	AT-9800
CR00012594	STT	3	With unidirectional traffic or small frames, an STT connection would sometimes stop passing data. This issue has been resolved.	Y	Y	Y	Y	-	-	-	-	-	-

## Level 4

CR	Module	Level	Description	AR44x / AR450	AR7x5	AR750S	Rapier i	AT-8800	AT-8600	AT-8700XL	AT-8948	AT-9900	AT-9800
CR00003286	Core, ISDN	4	Previously, the log message generated when an ISDN call came up sometimes reported the channel as “channel unknown” when the channel was encoded as a channel map instead of a channel number. The type of encoding depends on the local ISDN provider, so this issue only occurred in some parts of the world. This issue has been resolved. When the channel has been encoded as a channel map, the log message now displays one of the following: <ul style="list-style-type: none"> <li>■ a channel number if only one channel is encoded (the most common case), or</li> <li>■ the entire channel map in decimal format if more than one channel is encoded, for example:  28 11:51:21 3 ICC CALL UP ISDN call ACTIVE, direction IN , channel map 12.</li> </ul>	Y	Y	Y	Y	-	-	-	-	-	-

CR	Module	Level	Description	AR44x / AR450	AR7x5	AR750S	Rapier i	AT-8800	AT-8600	AT-8700XL	AT-8948	AT-9900	AT-9800
CR00011995	BGP	4	To simplify displaying BGP memory usage, the command <b>show bgp memlimit bgp</b> has been removed. Use the command <b>show bgp memlimit scan</b> instead. Also, you can now display only the BGP backoff log messages by using either of the following commands:  <pre>show log type=55 subtype=backoff</pre> <pre>show log type=55 subtype=7</pre>	Y	Y	Y	Y	Y	-	-	Y	Y	Y
CR00012043	BGP	4	When a user entered conflicting values for BGP backoff thresholds (the <b>backoff</b> and <b>low</b> parameters of the <b>set bgp backoff</b> command), the error message did not adequately show the dependency between these two parameters.  This issue has been resolved. The error message now reads (for example):  <pre>Error (3103332): BACKOFF parameter value 90 too low; must be greater than LOW parameter value 94.</pre>	Y	Y	Y	Y	Y	-	-	Y	Y	Y



## Enhancements

CR	Module	Level	Description	AR44x / AR450	AR7x5	AR750S	Rapier i	AT-8800	AT-8600	AT-8700XL	AT-8948	AT-9900	AT-9800
CR00007105	MSTP	-	<p>Two new commands have been added to simplify MSTP management:</p> <pre>enable mstp port={port-list all} disable mstp port={port-list all}</pre> <p>These commands enable or disable MSTP on the specified ports for the CIST and all currently-configured MSTIs, in a single step.</p> <p>Previously, this operation required two commands. For example, you can now use <b>enable mstp port={port-list all}</b> instead of the following commands:</p> <pre>enable mstp cist port={port-list all} enable mstp msti=instance port={port-list all}</pre>	-	-	-	Y	Y	Y	Y	Y	Y	-
CR00009825	IP Gateway	-	<p>When a router or switch receives a packet and does not have an ARP entry for the destination address, it broadcasts an ARP Request message over the egress IP interface. If it does not receive a reply within a short time, it notifies the sending device that the destination was unknown.</p> <p>This enhancement lets you configure how long the router or switch waits for a response. Use the following new command to specify the timeout period in seconds:</p> <pre>set ip arpwaittimeout=1..30</pre> <p>The default is 1 second. You may need to increase the timeout period if you are communicating with devices that are slow to respond.</p> <p>The easiest way to see the effect is to ping an unavailable device. The timeout determines the delay between pinging an IP address and receiving the reply that the device is unreachable.</p>	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR00011164	Switch	-	Improvements have been made to the throughput of AT-9924T/4SP switches when the AT-ACC01 accelerator card is installed.	-	-	-	-	-	-	-	-	Y	-

CR	Module	Level	Description	AR44x / AR450	AR7x5	AR750S	Rapier i	AT-8800	AT-8600	AT-8700XL	AT-8948	AT-9900	AT-9800
CR00011204	IP Gateway	-	This Software Version allows you to add ARP entries with multicast MAC addresses and allows the router or switch to accept packets with conflicting IP and MAC addresses. It introduces the <b>enable ip macdisparity</b> and <b>disable ip macdisparity</b> commands to support this. For more information, see <a href="#">“Adding Static ARP Entries with Multicast MAC Addresses (CR00011204)”</a> on page 37.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR00011271	Switch, Utility	-	A new switch filter feature enables you to use a switch filter to make a VLAN secure without preventing access to other VLANs. For more information, see <a href="#">“Securing a Single VLAN through Switch Filters (CR00011271)”</a> on page 39.	-	-	-	Y	Y	Y	Y	-	-	-
CR00011565	ASYN	-	When an asynchronous port is in <i>ten mode</i> , it bundles together the characters that it receives within a certain time period, instead of passing them one at a time to a higher protocol layer for processing. The time period over which characters are bundled is called the <i>ten timer</i> . This enhancement enables you to reduce the length of the ten timer, to improve response times for remote terminal sessions. For more information, see <a href="#">“Making Asynchronous Ports Respond More Quickly (CR00011565)”</a> on page 41.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR00011615	Switch	-	When a switch port has been given a description, it is now possible to use an SNMP application to see the port description, through the Interfaces group of the MIB-II MIB ifDescr OID.	Y	-	Y	Y	Y	Y	Y	Y	Y	Y
CR00011724	BGP	-	You can now display: <ul style="list-style-type: none"> <li>the number of routes learned from a specific peer, by using the existing command <b>show bgp peer=ip-address</b></li> <li>information about each route learned from a specific peer, by using the new <b>peer</b> parameter in the command <b>show bgp route peer=ip-address</b></li> </ul> For more information see <a href="#">“Displaying Routes Learned from a Specific BGP Peer (CR00011724)”</a> on page 43.	Y	Y	Y	Y	Y	-	-	Y	Y	Y

CR	Module	Level	Description	AR44x / AR450	AR7x5	AR750S	Rapier i	AT-8800	AT-8600	AT-8700XL	AT-8948	AT-9900	AT-9800
CR00012620	Bridging	-	<p>By default, when the router receives a tagged packet on an Eth or VLAN interface and bridges it, the bridge strips out the packet's VLAN tag. This enhancement enables you to set the bridge to instead retain the tag, by using <b>off</b>, <b>no</b> or <b>false</b> in the new command:</p> <pre>set bridge stripvlantag={on off yes no true false}</pre> <p>The default is <b>on</b>. To see whether stripping is turned on or off, use the command:</p> <pre>show bridge</pre> <p>and check the new <b>StripVlantag</b> entry.</p>	Y	Y	Y	-	-	-	-	-	-	-
CR00012692	L2TP	-	<p>The connection between the router or switch, acting as an LNS, and a third party peer, acting as an LAC, can sometimes fail during PPP link negotiation. Frequent negotiation failures can indicate a compatibility problem between the third party peer and Proxy Authentication responses from the router or switch. With this enhancement, you can now disable Proxy Authentication on the router or switch for situations where the third party equipment is not compatible. Use <b>proxyauth=off</b> in the command:</p> <pre>add l2tp ip=ipadd[-ipadd] pptemplate=0..31 [number={off on startup}] [pre13={off on}] [proxyauth={off on}] [tosreflect={off on false true no yes}]</pre> <p>The default for <b>proxyauth</b> is <b>on</b>. Proxy Authentication should not be disabled unless necessary.</p> <p>To see whether Proxy Authentication is turned on or off, use the command:</p> <pre>show l2tp ip</pre> <p>and check the new <b>Proxy Authentication</b> entry.</p>	Y	Y	Y	Y	Y	-	-	Y	Y	Y

## Features in 276-01

Software Maintenance Version 276-01 includes the resolved issues and enhancements in the following tables. In the tables, for each product series:

- “Y” in a white column indicates that the resolution is available in Version 276-01 for that product series.
- “-” in a white column indicates that the issue did not apply to that product series.
- a grey-shaded column indicates that Version 276-01 was not released on that product series.  
 “-” in a grey column indicates that the issue did not apply to that product series.  
 “Y” in a grey column indicates that the issue applied to that product series. These issues are resolved in the next Version (276-02).

### Level 1

No level 1 issues

### Level 2

CR	Module	Level	Description	AR400	AR7x5	AR750S	Rapier i	AT-8800	AT-8600	AT-8700XL	AT-8948	AT-9900	AT-9800
CR00008046	PPP	2	Previously, if the switch was acting as a PPPoE access concentrator, it was forwarding the first received ICMP Echo Request packet destined for a PPPoE client back to the sender. This has been resolved so the forwarding does not occur.	-	-	-	Y	Y	-	-	Y	Y	Y
CR00008244	Switch	2	When a user entered the command <b>disable switch port automdi</b> and saved the configuration with the <b>create config</b> command, the resulting configuration file did not include that command. This issue has been resolved.	-	-	-	-	-	-	-	Y	Y	-

CR	Module	Level	Description	AR400	AR7x5	AR750S	Rapier i	AT-8800	AT-8600	AT-8700XL	AT-8948	AT-9900	AT-9800
CR00008742	Switch	2	Previously, if a switch port's learn limit was changed to a number that was less than the currently-learned number of MAC addresses, you were unable to delete the learned MAC addresses. The switch also did not lock the port.  This issue has been resolved. The switch now deletes all learned MAC addresses and starts learning again.	-	-	-	Y	Y	Y	Y	Y	Y	Y
CR00008791	PIM	2	Previously, Layer 2 switching of multicast traffic did not always operate correctly when Layer 2 and Layer 3 multicast were being used at the same time.  This issue has been resolved.	-	-	-	Y	Y	-	-	Y	Y	Y
CR00009236	BGP	2	For BGP prefixes learned from an external EBGP peer, which were subsequently distributed within the router or switch's own AS via Route Reflection, the teaching time to the IBGP peers was excessively slow.  This issue has been resolved.	Y	Y	Y	Y	Y	-	-	Y	Y	Y
CR00009386	SSH	2	Previously, when the router or switch had encryption hardware installed, a slow memory leak occurred after multiple consecutive SSH connections were established.  This issue has been resolved.	-	Y	-	Y	-	-	-	-	-	-
CR00010232	STP	2	STP and RSTP did not work correctly when a static MAC filter was added.  This issue has been resolved, so that control traffic is not incorrectly discarded in the presence of configured switch filters. Also, configured switch filters are now applied to locally generated control traffic.	-	-	-	Y	Y	Y	Y	Y	Y	Y
CR00010278	IP	2	Multihomed IP interface addresses could not be used as the default local IP address.  This issue has been resolved.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR00010307	Switch	2	Invalid entries were sometimes added to the hardware IP table.  This issue has been resolved.	-	-	-	-	-	-	-	Y	Y	-

CR	Module	Level	Description	AR400	AR7x5	AR750S	Rapier i	AT-8800	AT-8600	AT-8700XL	AT-8948	AT-9900	AT-9800
CR00010539	IP	2	Sometimes the forwarding of packets occurred unnecessarily slowly. This happened if the forwarding interface was associated with an IP filter with a variable field pattern, such as TCP session or ICMP code and type.  For switches, note that this issue occurred when the switch was routing IP packets in software, and had no effect on the hardware forwarding of packets.  This issue has been resolved.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR00010784	Switch	2	Previously, if a 48-port switch was configured with one or more port-specific hardware filters, followed by one or more non port-specific hardware filters, then the non port-specific filter was not correctly applied to half of the ports on the switch.  This issue has been resolved by defining the following new command, which enables you to decide which mode you want the hardware filters to operate in: set switch hwf mode={psf npsf} where: psf = port specific first (default mode) npsf = non port-specific first If the first filter is non port-specific, set the mode to <b>npsf</b> .	-	-	-	Y	Y	Y	Y	-	-	-
CR00010888	Port Authentication	2	When 802.1x port authentication was configured in multi-supPLICANT mode, supplicants with EAP-TLS, PEAP-MS-CHAPv2 or PEAL-TLS authentication methods were not able to access the network.  This issue has been resolved.	Y	Y	Y	Y	Y	Y	Y	Y	Y	-
CR00010890	PPP	2	For a PPP interface over an ACC call, RADIUS accounting messages were not being sent.  This issue has been resolved.	Y	Y	Y	Y	Y	-	-	-	-	-
CR00010896	Switch	2	AT-40/SC, AT-40/MT and AT-41/MT uplink modules would stay link down when they were set to a fixed speed.  This issue has been resolved.	-	-	-	Y	-	-	Y	-	-	-

CR	Module	Level	Description	AR400	AR7x5	AR750S	Rapier i	AT-8800	AT-8600	AT-8700XL	AT-8948	AT-9900	AT-9800
CR00010996	Port Authentication	2	When port authentication was using a RADIUS server, it sometimes stopped working after several hours. This was because port authentication generated RADIUS Accounting Request (STOP) messages with an incorrect Acct-Session-Time value. This issue has been resolved.	Y	Y	Y	Y	Y	Y	Y	Y	Y	-
CR00011040	Ping	2	When the router or switch was configured with multiple logical interfaces, it chose the source address of the ICMP Echo Reply incorrectly in some configurations. This issue has been resolved.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR00011068	SSL	2	Previously, there was a memory corruption issue in the SSL client and server implementation. This issue has been resolved.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR00011111	IPX	2	Forwarding an 802.3 or ETHII encapsulated IPX packet over a VLAN to a remote network occasionally caused the switch to reboot. This issue has been resolved.	-	-	-	Y	Y	Y	Y	Y	Y	Y
CR00011213	PIM 6	2	Previously, the switch treated a valid bootstrap message as a bad message if it received the message on two or more interfaces, and when PIM6 operated in a looped or network topology that had multiple unicast routes to the same destination(s), it sometimes selected a sub-optimal route for RPF interface selection for RP and BSR elections. This issue has been addressed by an additional algorithm to deal with equal cost multipath routes as follows: a. if more than one route to the same given destination with equal cost exists, then the route with highest nexthop IP address value will be selected. b. if the nexthop IP address values are the same (the routes come from the same device on different interfaces), then the routes with highest interface index will be selected.	Y	Y	Y	Y	Y	-	-	Y	Y	Y

CR	Module	Level	Description	AR400	AR7x5	AR750S	Rapier i	AT-8800	AT-8600	AT-8700XL	AT-8948	AT-9900	AT-9800
CR00011243	ISAKMP	2	Previously, if an IPsec/ISAKMP tunnel was under heavy load, an ISAKMP peer may have retransmitted messages. When the last message in an ISAKMP exchange was retransmitted, the remote peer did not expect to receive the second message after the exchange had finished and caused the router or switch to reboot. This issue has been resolved.	Y	Y	Y	Y	Y	-	-	-	-	-
CR00011269	SSL	2	When the SSL server had multiple concurrent users, some SSL sessions failed to establish, because the SSL handshakes failed. This issue has been resolved.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR00011300	User	2	Previously, if the router or switch was acting as an 802.1x authenticator, and it received an illegal RADIUS packet (an Access-Reject packet with an EAP code of “successful”), the router or switch would reboot. This issue has been resolved. The switch now rejects such authentication requests.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR00011324	SSL	2	A reboot could occur when the SSLv2 client received a hello message that had an incorrect challenge length. This issue has been resolved, so that the SSL server’s resistance to denial of service attacks has been improved.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR00011328	PIM	2	When the switch was using PIM to route multicast traffic, it sometimes rebooted if the command <b>show switch table=nh</b> was entered. This issue has been resolved.	-	-	-	-	-	-	-	Y	Y	-
CR00011337	Environment Monitoring	2	The switch did not record the system temperature, and therefore output of the command <b>show system</b> displayed the temperature as 0°C. This issue has been resolved.	-	-	-	-	-	-	-	-	-	Y
CR00011345	MIB	2	The ATR enterprise MIB includes objects for managing ping operations. These objects within the MIB are now fully supported. Minor modifications have also been made to the MIB. Download the latest attrouter.mib file from <a href="ftp.alliedtelesyn.co.nz/pub/ar-mib/atrouter.zip">ftp.alliedtelesyn.co.nz/pub/ar-mib/atrouter.zip</a> .	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y



CR	Module	Level	Description	AR400	AR7x5	AR750S	Rapier i	AT-8800	AT-8600	AT-8700XL	AT-8948	AT-9900	AT-9800
CR00011387	PPP	2	Using an online limit for a PPP interface over PPPoE over a VLAN caused the router or switch to reboot when the online limit was reached. This issue has been resolved.	Y	Y	Y	Y	Y	-	-	Y	Y	Y
CR00011402	SSL	2	Previously, if an SSL client closed the TCP connection before the SSL handshake was complete then the SSL server was not forwarding the notification onto HTTP. The TCP session was left in the close wait state and HTTP, SSL and TCP sessions did not time out. This issue has been resolved.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR00011473	ISAKMP	2	Configuring an ISAKMP policy with a 24-character name sometimes caused the router or switch to reboot. Also, it was possible to enter over-length names into the <b>isakmppolicy</b> parameter of the command <b>set ipsec policy</b> . Both issues have been resolved.	Y	Y	Y	Y	Y	-	-	-	-	-
CR00011585	OSPF	2	Adding the same OSPF stub or host twice caused OSPF to suspend its operation, causing neighbour relationships to eventually fail. This issue has been resolved.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR00011611	IP Multicast	2	The router or switch did not forward multicast traffic addressed to 239.255.255.250, even when the router or switch was not involved with UPnP service discovery. This issue has been resolved. The router or switch now forwards the specified multicast traffic unless UPnP is enabled.	Y	Y	Y	Y	Y	-	-	Y	Y	Y
CR00011660	DHCP snooping	2	Previously, setting a port's trusted state to true twice in succession would cause the switch to reboot. This issue has been resolved.	-	-	-	Y	Y	Y	Y	Y	Y	-
CR00011666	CORE	2	AR745 routers sometimes had a high CPU utilisation after restarting, although they were idle. This issue has been resolved.	-	Y	-	-	-	-	-	-	-	-
CR00011727	UPNP	2	Deleting a firewall policy that UPnP was using could cause the router to reboot.	Y	Y	Y	-	-	-	-	-	-	-

## Level 3

CR	Module	Level	Description	AR400	AR7x5	AR750S	Rapier i	AT-8800	AT-8600	AT-8700XL	AT-8948	AT-9900	AT-9800
CR00006439	GUI	3	When a user logged onto the router or switch through the GUI, the router or switch's log recorded several HTTP 404 (Not Found) errors. This was because the browser expected to see some images that the GUI resource file did not contain. This issue has been resolved. The expected images are now present.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR00011055	Classifier	3	If a user attempts to change the range of TCP or UDP ports used by a classifier, the hardware filter table may not be updated if there is a lack of hardware filter table space. Previously, this resulted in a mismatch between the hardware and software filter tables.  This issue has been resolved, such that if the port range change is not possible, both the software and hardware filter tables revert back to the original filter definitions.	-	-	-	-	-	-	-	Y	Y	-
CR00011123	IP Multicast	3	Previously, the switch dropped a multicast packet if the packet had IP options bits set and the switch had recently forwarded multicast data to the group address in the packet.  This issue has been resolved.	-	-	-	Y	Y	-	-	Y	Y	Y
CR00011482	Firewall	3	The parameters <b>maxupnpportmap</b> and <b>icmpunreachbletimeout</b> were missing from the command <b>set firewall policy</b> .  This issue has been resolved.	Y	Y	Y	Y	Y	-	-	-	-	Y
CR00011550	IP multicast	3	Performance of the switch's internal manipulations of IP multicast routes has been improved, and the stability of PIM-DM under extremely high loads has correspondingly been improved.	-	-	-	-	-	-	-	Y	Y	-
CR00011609	DHCP snooping	3	A new lease could be added to the DHCP snooping database as a full entry even after the maximum number of leases for the port had been exceeded.  This issue has been resolved.	-	-	-	Y	Y	Y	Y	Y	Y	-

CR	Module	Level	Description	AR400	AR7x5	AR750S	Rapier i	AT-8800	AT-8600	AT-8700XL	AT-8948	AT-9900	AT-9800
CR00011664	PERM	3	The IAC (interpret as control) characters (0xFF) are escaped when sent across the permanent assignment connection. If TCP could not send the entire buffer, the two IAC characters were previously split up, which resulted in extra IAC characters in the receive buffers.  This issue has been resolved. IAC characters and their escape are no longer split over buffers.	Y	Y	Y	-	-	-	-	-	-	-
CR00011739	IP	3	Previously, a route map entry could not be deleted if the route map was used by BGP, OSPF or RIP. Now the route map entry can be deleted unless it is the last entry of the route map.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR00011754	VRRP	3	Previously, when a ping was sent to the virtual router address of a VRRP pair, and VR IP address adoption was turned on ( <b>adopt=on</b> ), the reply message was sent back from the IP address of the interface that was being used, instead of from the IP address of the virtual router that was pinged. Some systems failed the ping because of this address mismatch.  This issue has been resolved. Ping replies now come from the IP address of the virtual router that was pinged.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y

## Level 4

CR	Module	Level	Description	AR400	AR7x5	AR750S	Rapier i	AT-8800	AT-8600	AT-8700XL	AT-8948	AT-9900	AT-9800
CR00011004	QoS	4	Previously, if you used the ? or Tab keys to obtain help about the Quality of Service commands, the resulting help included references to RED curves, which are not available on the switch.  This issue has been resolved—the help no longer refers to RED curves.	-	-	-	Y	Y	Y	Y	-	-	-
CR00011056	Classifier	4	Previously, it was possible to create multiple classifiers that classified packets according to the same UDP or TCP port range.  This issue has been resolved. If you attempt to create such a classifier, the switch displays an error message.	-	-	-	-	-	-	-	Y	Y	-

## Enhancements

CR	Module	Level	Description	AR400	AR7x5	AR750S	Rapier i	AT-8800	AT-8600	AT-8700XL	AT-8948	AT-9900	AT-9800
CR00010196	BGP, IP gateway, Switch	-	A new feature enables you to set the maximum length of the hardware route update queue, and display the current queue size, status and maximum length. For more information, see <a href="#">"Route Update Queue Length (CR00010196)" on page 44.</a>	-	-	-	-	-	-	-	Y	Y	-
CR00011355	PERM	-	Support for permanent assignments has been added to the router. Permanent assignments provide a method for creating permanent links between terminal ports on routers. For information and command syntax, see <a href="#">"Permanent Assignments (CR00011355)" on page 46.</a>	Y	-	-	-	-	-	-	-	-	-
CR00011614	ASYN	-	Support for baud rates of 300, 600, 1200 and 2400 has been added to the ports on the AR024 PIC. This PIC provides 4 asynchronous ports.	Y	Y	Y	Y	-	-	-	-	-	-

# Adding Static ARP Entries with Multicast MAC Addresses (CR00011204)

---

This Software Version allows you to add ARP entries with multicast MAC addresses and allows the router or switch to accept packets with conflicting IP and MAC addresses. It introduces the **enable ip macdisparity** and **disable ip macdisparity** commands to support this.

## Adding Static ARP Entries

Valid ARP entries are normally restricted to unicast IP with unicast MAC addresses. However, ARP entries can be configured with multicast MAC addresses when **macdisparity** is enabled. Static ARP entries with multicast MAC addresses are necessary for some third party networking solutions, such as server clustering.

Before you can add an ARP entry with a multicast MAC address, you must enable **macdisparity** using the command:

```
enable ip macdisparity
```

Once this feature is enabled, you can add an ARP entry with a multicast MAC address using the **add ip arp** command.

## Accepting Packets with Conflicting Addresses

Enabling **macdisparity** also allows the router or switch to accept packets with conflicting IP and MAC addresses. Normally the router or switch discards these packets as being invalid.

Conflicting IP and MAC addresses include:

- A multicast IP address with a unicast MAC address
- A unicast IP address with a multicast MAC address

**Macdisparity** is disabled by default. When disabled, only ARP entries with unicast IP and MAC addresses can be added, and packets with conflicting addresses are discarded. Other routers or switches in the network may not accept packets with conflicting addresses unless configured to. To disable this functionality, use the command:

```
disable ip macdisparity
```

ARP entries with multicast MAC addresses must be removed before the **disable ip macdisparity** command will work. To see details on the current ARP entries, use the command:

```
show ip arp
```

To see whether **macdisparity** is enabled or disabled, use the command:

```
show ip
```

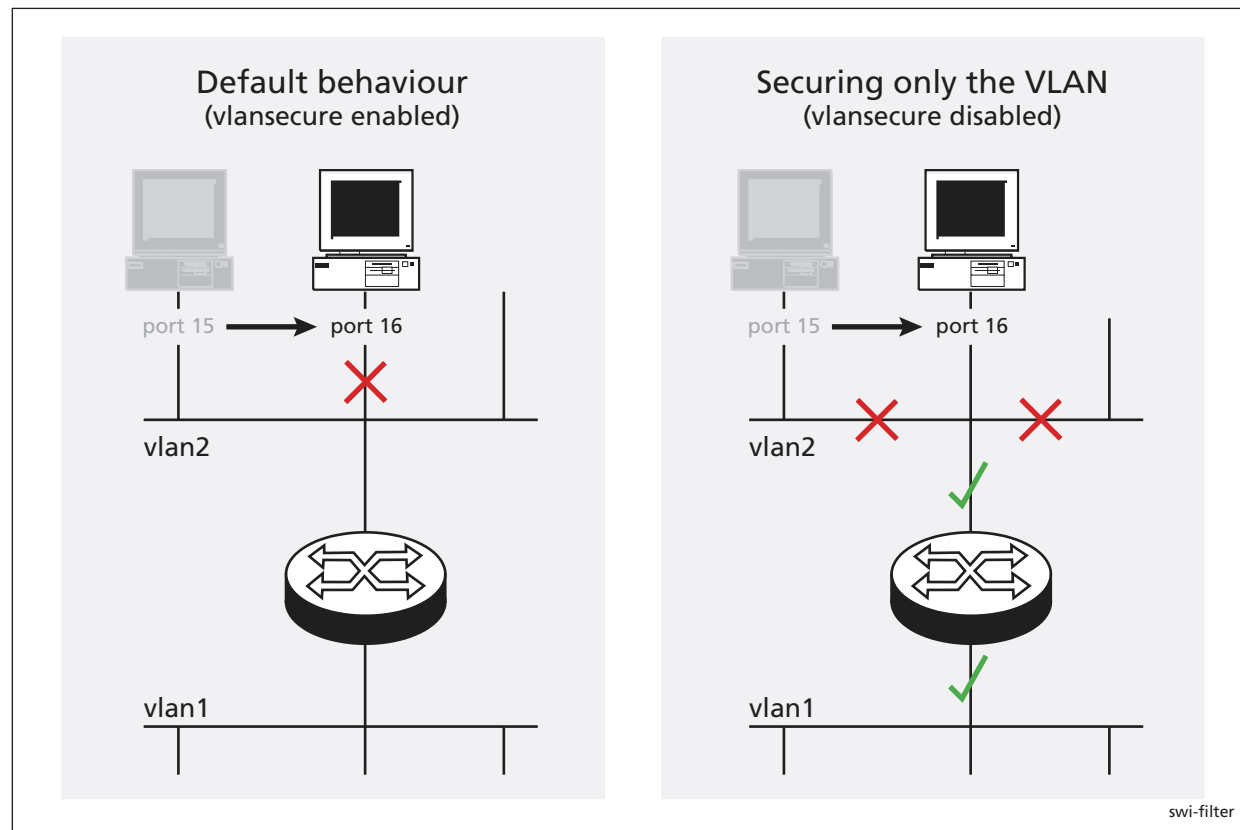
For an example of how to use ARP entries with multicast MAC addresses, see *Guideline to Windows 2003 Network Load Balancing Clustering with Allied Telesyn Switches*. This is available from the Resource Center on your Documentation and Tools CD-ROM, or from:  
[www.alliedtelesyn.co.uk/en-gb/solutions/techdocs.asp?area=howto](http://www.alliedtelesyn.co.uk/en-gb/solutions/techdocs.asp?area=howto)

## Securing a Single VLAN through Switch Filters (CR00011271)

On AT-8824, Rapier 24i, AT-8724XL and AT-8624 switches, this enhancement enables you to use switch filters to secure only the current VLAN, instead of securing all VLANs on the switch. To turn on this feature, a new command disables “vlansecure” for filters (see [“Configuring vlansecure” on page 40](#)). Without this enhancement (the default situation) a switch filter only allows a host to access the network through a particular port on the switch. For example, if you have a PC connected to port 15 in vlan2, and define the following filter, the PC can only communicate when it is connected to port 15:

```
add switch filter entry=0 dest=pc-mac-address vlan=2 port=15 action=forward
```

With this enhancement, the above filter limits the host to accessing vlan2 through port 15, but does not prevent the host from accessing other VLANs through other ports in vlan2. For example, if the above filter exists and you move the PC to another port in vlan2, this enhancement prevents the PC from communicating with devices in vlan2 but allows it access to other VLANs on the switch. The following figure shows a PC that has been moved from port 15 to port 16 to illustrate the effect.



## Configuring vlansecure

To turn off the default behaviour, so that the filter prevents access to only the current VLAN when you move the host, use the new command:

```
disable switch filter vlansecure
```

To return to the standard filter behaviour, use the new command:

```
enable switch filter vlansecure
```

To display which mode the filtering behaviour is in, use the existing command:

```
show switch filter
```

This command now displays the additional field “VlanSecure”, which is either DISABLED or ENABLED.



## Making Asynchronous Ports Respond More Quickly (CR00011565)

---

When an asynchronous port is in *ten mode*, it bundles together the characters that it receives within a certain time period, instead of passing them one at a time to a higher protocol layer for processing. The time period over which characters are bundled is set by the *ten timer*.

Bundling reduces the load on the CPU by spreading the character processing overhead across several characters. If a remote terminal session is involved, bundling also reduces the number of packets on the network by sending more characters in each packet. However, it reduces terminal responsiveness. A ten timer value of 100 milliseconds is generally a good compromise between responsiveness and processing overhead. If you need to increase the port's responsiveness, this enhancement enables you to reduce the length of the ten timer. To do this, use the new optional **tentimervalue** parameter in the **set asyn** command:

```
set asyn[=port-number] tentimervalue=20..100 [other optional parameters]
```

Specify the asynchronous port number unless you are logged in via the port you want to change.

The default **tentimervalue** is 100 milliseconds, which is the value it was set to before this enhancement.

To display a port's value for the ten timer, use the command:

```
show asyn=port-number
```

and check the new "Ten timer value" field, as shown in [Figure 1](#). If the asynchronous port is a terminal server port in ten mode, the "Mode" field displays "Ten".

Figure 1: New parameters in the output of the **show asyn=0** command

```
ASYN 0 : 0000001470 seconds    Last change at: 0000001465 seconds

ASYN information
Name ..... Asyn 0
Status ..... enabled
Mode ..... Ten
Data rate ..... 9600
Parity ..... none
Data bits ..... 8
Stop bits ..... 1
Test mode ..... no
In flow state (mode) ..... on (Hardware)
Out flow state (mode) ..... off (Hardware)
Autobaud mode ..... disabled
Max tx queue length ..... 16
TX queue length ..... 3
Transmit frame ..... none
RX queue length ..... 0
IP address ..... none
Max transmission unit ..... 1500
Ten timer value ..... 100
.
.
.
```

## Displaying Routes Learned from a Specific BGP Peer (CR00011724)

---

This enhancement enables you to display:

- the number of routes learned from a specific peer
- information about each route learned from a specific peer

### Displaying the Number of Routes from a Peer

To display the number of routes learned from a specific peer, use the existing command:

```
show bgp peer=ip-address
```

and check the new “Routes learned” field ([Figure 2](#)).

Figure 2: New parameter in the output of the **show bgp peer** command for a specific peer

```
Peer ..... 192.168.10.1
Description ..... -
State ..... Idle
Policy Template ..... 4
Description ..... Test Template 1
Private AS filter ... Yes
Remote AS ..... 3
BGP Identifier ..... 172.20.25.2
Routes learned ..... 15
Authentication ..... None
Password ..... -
.
.
.
```

### Displaying Information about the Routes from a Peer

To display information about each route learned from a specific peer, use the new **peer** parameter in the command:

```
show bgp route[=prefix] [peer=ip-address] [other optional parameters]
```

The **peer** parameter specifies the IP address of the peer. If you specify a peer, the router or switch only displays routes that it learned from that peer. If you specify the router or switch’s router ID, it displays all locally originated routes. The **peer** parameter has no default.

Note that this enhancement did not change any fields in the output of the **show bgp route** command; it simply provides another method of filtering the displayed routes.

## Route Update Queue Length (CR00010196)

When hardware learning delay is enabled (the default), the switch learns new routes in software, then places them into a queue for adding them to its hardware routing table. Defaults have been set for the maximum number of entries in the queue, and depend on the amount of memory installed on the switch, as shown in the following table:

Memory Size (Mbytes)	Default length (number of entries)	Maximum possible length (number of entries)
up to 128	200000	200000
129-256	1000000	1500000
more than 256	3000000	4000000

You can alter the length of the queue, by using the following new command to specify the maximum number of entries in the queue:

```
set switch hwrouteupdate=1..maximum
```

The *maximum* depends on the amount of memory on the switch, as shown in the table above.

Output of the **show switch** command has been expanded to display information about the queue settings ([Figure 3](#), [Figure 4](#), [Table 1](#)).

Figure 3: Output of the **show switch** command when hardware learning delay is disabled

```
Switch Configuration
-----
Switch Address ..... 00-00-cd-12-78-03
Learning ..... ON
Ageing Timer ..... ON
IP route:
  Learn delay ..... OFF
    queue limit ..... 1000000
    queue maximum ..... 1500000
    queue default ..... 1000000
  Updating hardware(status) 0 (Pending)
.
.
.
```

Figure 4: Output of the **show switch** command when hardware learning delay is enabled

```

Switch Configuration
-----
Switch Address ..... 00-00-cd-12-78-03
Learning ..... ON
Ageing Timer ..... ON
IP route:
  Learn delay ..... 4 ms
    queue size ..... 0
    queue limit ..... 1000000
    percent in use .... 0
    high water mark ... 0
    queue maximum ..... 1500000
    queue default ..... 1000000
  Updating hardware(status) 0 (Pending)
.
.
.

```

Table 1: New parameters in the output of the **show switch** command

Parameter	Meaning
Queue size	The number of entries currently in the hardware route update queue.
Queue limit	The maximum number of entries that the queue can hold.
Percent in use	The percentage of the queue limit that is currently used.
High water mark	The highest number of messages that have been seen on the queue since the switch last started up.
Queue maximum	The maximum value to which you can set the queue size. This depends on the amount of memory installed on the switch.
Queue default	The default maximum number of entries in the queue. This depends on the amount of memory installed on the switch.
Updating hardware (status)	The number of entries that the software has queued for writing into the hardware table, followed by the status. Status is Pending if the hardware is not currently processing queued routes and Active if it is currently processing the routes.

## Permanent Assignments (CR00011355)

---

Permanent assignments provide a method for creating permanent links between terminal ports on routers. Any two terminal ports on a single router or on routers that can communicate with each other via TCP/IP can be set up to have a permanent assignment between them. Asynchronous traffic coming into each port is sent via TCP to other port and then sent out that port.

The most common use of permanent assignments is to provide access to network printers. However, permanent assignments can connect any asynchronous devices together. Other examples include connecting a terminal to a host computer asynchronous port and connecting an asynchronous port on a data logger to a computer for capturing the results of experiments.

### Setting up a Permanent Assignment

To set up a permanent assignment, the port numbers of the ports and the IP addresses of the routers at each end of the link must be specified. Each permanent assignment is also given a name. The name is used for management convenience and for identification purposes when the permanent assignment's TCP connection is made at router boot or when the permanent assignment is created or reset. A short dialogue takes place between the two routers involved in the permanent assignment when the assignment is set up, to verify that the correct ports are being connected. This dialogue uses the permanent assignment name for verification. The name is case sensitive and must be identical for both ends of the permanent assignment.

Each end of the permanent assignment must be set up for the assignment to work correctly. A common cause of problems for permanent assignments is one end of the assignment being set up incorrectly.

A given permanent assignment has a different view looking from each end of the assignment. The terms *local* and *remote* are used to denote the ends of the assignment from one point of view. Thus there is a local and remote port and a local and remote router for each permanent assignment. Note that the local router is the router that the command is being entered on.

To set up one end of a permanent assignment use the command:

```
add perm=name
```

The name of the permanent assignment, the local and remote ports and the IP address of the remote router must all be specified in this command.

To display the configuration of the permanent assignment ([Figure 5](#)), use the command:

```
show perm
```

Figure 5: Example output from the **show perm** command

Name	Port		IP address
	Local	Remote	
laser-print	12	04	172.16.8.37

If the two ports of the permanent assignment are on different routers, the **add perm** command must be entered on each router. If both ports are on the same router, the command only needs to be entered once. The IP address specified may be any one of the IP addresses of the router in question.

A permanent assignment can be removed with the command:

```
delete perm=name
```

This command removes the permanent assignment from the local router. If the other port of the permanent assignment is on a remote router, the permanent assignment should also be removed from the remote router.

A permanent assignment can be reset with the command:

```
reset perm
```

This command breaks the current TCP connection being used for the permanent assignment and attempts a new connection. The terminal port being used for the permanent assignment is also reset.

## Example

This example illustrates the process of setting up a permanent assignment. The assignment is to be established between port 2 on a router with IP address 172.26.4.1 and port 2 on a router with IP address 172.20.34.9, and is to be named main office. The commands to be executed on the router with address 172.26.4.1 are:

```
add perm=main office lport=2 rport=3 ip=172.20.34.9
show perm
```

which produces the output shown in [Figure 6](#).

Figure 6: Example output from the **show perm** command for router 172.26.4.1

Name	Port		IP address
	Local	Remote	
main office	02	03	172.20.34.9

The commands to be executed on the router with address 172.20.34.9 are:

```
add perm="main office" lport=3 rport=3 ip=172.26.4.1
show perm
```

which produces the output shown in [Figure 7](#).

Figure 7: Example output from the **show perm** command for router 172.20.34.9

Name	Port		IP address
	Local	Remote	
main office	03	02	172.26.4.1

Since the name of the permanent assignment in this example contains embedded spaces, the whole name must be in double quotes when entered in a command.



## Command Reference

This section describes commands available on the router to configure and manage permanent assignments.

### add perm

---

#### Syntax

```
ADD PERM=perm-name LPORT=lport RPORT=rport IP=ipadd
```

where:

- *perm-name* is the name of the permanent assignment. The name is case-sensitive and must be identical on each router in the permanent assignment. If the name contains spaces, it must be in double quotes.
- *lport* is the number of the local asynchronous port for this permanent assignment. Ports are numbered sequentially starting with port 0.
- *rport* is the number of the remote asynchronous port for this permanent assignment. Ports are numbered sequentially starting with port 0.
- *ipadd* is the IP address of the remote router.

#### Description

This command adds one end of a permanent assignment. The permanent assignment must be specified by name, and the local and remote terminal ports and the IP address of the remote router must be specified.

The local and remote ends of a permanent assignment must be configured with the same name. Each permanent assignment on a given router must be configured with a different name.

#### Examples

To add a permanent assignment called *DataLogger* between port 1 on the local router and port 1 on a remote router with the IP address 172.16.38.5, use the command:

```
add perm=datalogger lport=1 rport=1 ip=172.16.38.5
```

## Related Commands

[delete perm](#)  
[reset perm](#)  
[set perm](#)  
[show perm](#)

## delete perm

---

### Syntax

```
DELEte PERM=perm-name
```

where *perm-name* is the name of the permanent assignment. The name is case sensitive and must be identical on each router in the permanent assignment. If the name contains spaces, it must be in double quotes.

### Description

This command removes a named permanent assignment from the local router. The permanent assignment must also be removed from the remote router.

### Examples

To delete the permanent assignment called *DataLogger*, use the command:

```
del perm=datalogger
```

## Related Commands

[add perm](#)  
[reset perm](#)  
[set perm](#)  
[show perm](#)

## reset perm

---

### Syntax

```
RESET PERM=perm-name
```

where *perm-name* is the name of the permanent assignment. The name is case sensitive and must be identical on each router in the permanent assignment. If the name contains spaces, it must be in double quotes.

### Description

This command resets a named permanent assignment. The port being used by the permanent assignment is reset and the TCP connection being used for the permanent assignment is reset. A new TCP connection is established for the permanent assignment.

### Examples

To reset the permanent assignment called *DataLogger*, use the command:

```
reset perm=datalogger
```

### Related Commands

[add perm](#)  
[delete perm](#)  
[set perm](#)  
[show perm](#)

## set perm

---

### Syntax

```
SET PERM=perm-name [LPORT=lport] [RPORT=rport] [IP=ipadd]
```

where:

- *perm-name* is the name of the permanent assignment. The name is case sensitive and must be identical on each router in the permanent assignment. If the name contains spaces, it must be in double quotes.
- *lport* is the number of the local asynchronous port for this permanent assignment. Ports are numbered sequentially starting with port 0.
- *rport* is the number of the remote asynchronous port for this permanent assignment. Ports are numbered sequentially starting with port 0.
- *ipadd* is the IP address of the remote router.

### Description

This command changes the configuration of an existing permanent assignment. The permanent assignment must be specified by name. At least one other parameter must be specified.

The remote end of the permanent assignment must also be configured on the remote router.

### Examples

To change the local and remote asynchronous ports used by the permanent assignment called DataLogger to port 0, use the command:

```
set perm=datalogger lport=0 rport=0
```

### Related Commands

[delete perm](#)

[reset perm](#)

[show perm](#)

## show perm

---

### Syntax

```
SHOW PERM[=perm-name]
```

where *perm-name* is the name of a permanent assignment

### Description

This command displays the name, local and remote ports and remote IP address for all permanent assignments currently defined on the router. If a permanent assignment is specified by name, only that permanent assignment is displayed ([Figure 8](#), [Table 2](#)).

Figure 8: Example output from the **show perm** command

Name	Port		IP address
	Local	Remote	
laser-print	12	04	172.16.8.37

Table 2: Parameters in output of the **show perm** command

Parameter	Meaning
Name	Name of the permanent assignment.
Local	Local port for the permanent assignment.
Remote	Remote port for the permanent assignment.
IP address	IP address of the remote router.

### Examples

To display all the permanent assignments configured on the local router, use the command:

```
show perm
```

**Related Commands**

add perm  
delete perm  
reset perm  
set perm